Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials

Y. Ganesh Raj[1], G. Naresh[2], R. Likith[3], Dr.R.Varun[4]

[1,2,3]Scholar, Department of CSE in Jayamukhi institute of technological sciences, Narsampet, Warangal, Telangana, India

[4]Assistant professor, Department of CSE in Jayamukhi institute of technological sciences, Narsampet, Warangal, Telangana, India

ABSTRACT

Throughout full compliance with access policies, users who want to use services are often needed to give personally identifiable information such as their age, occupation, and location. This personal information is readily apparent in the implementation of e-ticketing, which allows users to get discounted entry to tourist sites or transportation services provided they fulfil regulations relating to their age, handicap, or other predefined over qualities. In order to ensure that users' personal information is kept confidential, our electronic ticketing system makes use of attribute-based credentials. The characteristics of a user are validated by having them validated by a reliable third party, which is one of the benefits of our scheme. This allows the scheme to give guarantees to a seller that the user's characteristics are legitimate. The following are some of the contributions made by the scheme: (1) users are able to buy distinct ticket online from event organisers without the exact attributes of those tickets being disclosed; (2) two tickets belonging to the same user cannot be linked; (3) a ticket cannot be transmitted to some other consumer; and (4) a ticket cannot be double spent. The innovative aspect of our plan is that it gives users the ability to anonymously purchase reduced tickets by persuading ticket sellers that their characteristics meet the requirements of the ticket regulations. This is a step towards defining an electronic ticketing system that captures the user privacy needs in transport companies, and it has been taken here. The safety of our plan has been shown, and its complexity has been reduced to a well-established premise.

I. INTRODUCTION

Electronic ticketing systems, often known as etickets, seem to be the subject of substantial study from both the commercial and academic research sectors [1, 2], [3], [4], [5] due to the adaptability and portability of these systems. [1], [2] E-tickets offer a number of benefits, including the elimination of paper costs (tickets can be kept on a hand-held device), an improvement in customer service (tickets can be purchased and delivered at any time and place), and a reduction in environmental impact (tickets can be stored on a hand-held device). However, the use of e-tickets also raises some interesting questions protects the confidentiality of its users. This is due to the fact that it is possible to link different e-ticket transactions to a specific user – in contrast to paper-based tickets, which are anonymous – and as a result, it has the potential to reveal private information, such as working patterns, likely places of work, and other such things.

Customers are becoming more conscious of concerns about their privacy, particularly in light of the recently implemented global data protection legislation (GDPR) [6]. One solution to

this problem is anonymous authentication, which provides users with the ability to authenticate themselves without disclosing their identities. This method has been implemented to safeguard the privacy of users in a number of privacy-preserving e-ticket schemes [3, [7], [8], [9], [10], and [11] respectively. Despite this, many of these strategies have not been shown to be secure by official testing. Exceptions that need special mention are the ones that were suggested by Arfaoui et al. [8] and Rupp et al. [12]. Arfaoui et al. [8] fully established their security models for e-ticket systems, including unforgeability, unlinkability, and non-repudiation; nevertheless, the authors only presented a very high-level proof for their models.

Rupp et al. [12] formalised their security models of colonial territories which was before without refunds schemes encompassing transportation authorities security as well as user privacy; nonetheless, the security evidence of their system was once again at a high level.

Another requirement for a realistic e-ticket system is the support for different tickets based on a user's attributes (such as age, location, disability, profession, and so on), for example, to offer discounts for students or disabled passengers. This is a requirement that must be met in order for the system to be considered realistic. When buying or validating tickets, however, there is the possibility of such a ticket system disclosing more information about a user than is strictly required. This danger exists only if the system is not correctly constructed. For instance, a student who purchases a student ticket at a discounted price might end up disclosing the school where she is currently enrolled and, depending on the student card, even her birthday; however, neither of these pieces of information is required in order to qualify for the student discount. The very minimum of evidence that is necessary is that she can show that she is enrolled in an accredited educational institution. In a similar vein, a passenger who is handicapped may be required to provide additional information regarding his or her condition to the person selling or confirming the ticket in order to complete the transaction successfully. This topic was discussed by Gudymenko [10] and Kerschbaum et al. [11], but the validity of their proposed solutions was not officially shown.

Because it is so simple to make a copy of an e-ticket, businesses that run transportation systems are understandably worried about the possibility of fraudulent use of these tickets. As a result, support for a feature known as double spend or, more broadly, overspend detection, which is the process of evaluating if a ticket has been spent an excessive number of times, is also an essential component that an e-ticket system should have.

This article presents a novel privacy-preserving e-ticket method employing attribute-based credentials that allows for the issuance of various tickets depending on a user's characteristics. The goal of this study is to satisfy the criteria that have been outlined above. Our system allows for the deanonymization of users who attempt to use their tickets more than once while maintaining the privacy of users who are honest about their intentions (double spend detection). It is also a general e-ticket system, and it can be utilised in a variety of application scenarios, such as the following: • mobility as a service transport tickets (such as rail, bus, etc.) where age, disability, profession, affiliation, etc. might determine the prices of tickets; • one-off token for Internet services (such as print service, download

service for multimedia, etc.) where age, affiliation, membership might determine the service/access level; • e-voting where age, nationality.

II. Related Work

Mut-Puigserver et al. conducted a survey of a large number of e-ticket systems and compiled a summary of their various functional functional requirements and security requirements. These functional requirements included things like an expiration date, functionality, versatility, and more. The security requirements included things like integrity, authentication, fairness, nonoverspending, anonymity, generalizability of the findings, unlinkability, and more.

E-ticketing systems may be broken down into a few distinct categories, including transferable tickets [5, 7], untransferable tickets [3], [13], multiuse tickets [3], [4], and single-use tickets [3, 5], [7], [14]. [3], [5], [7], [14]

Our plan involves non-refundable, one-time-use tickets, so they cannot be sold or traded.

Classifications while while guaranteeing anonymity, unlinkability, fiscal responsibility, and adaptability. In this part of the discussion, we will contrast our plan with a few other plans. Blind signatures [15], group signatures [16], anonymous credentials [17], and pseudonyms [16], [18] were employed to safeguard user privacy in these systems. [15]; [16]; [17]; [18]; [15]; [15]; [15]; [15]; [15]

Schemes for Electronic Tickets Generated from Blind Signatures In a system known as a blind signature, a user is able to receive a signature on a message without the signer being aware of the contents of the message. Based on the blind signature method developed by Chaum [15], Fan and Lei [19] presented an electronic ticket system for voting. In this system, each voter would only need one ticket to vote in all of the elections that they are eligible for. Song and Korba [9] came up with the idea of using an e-ticket system in pay-TV services in order to secure the consumers' privacy and offer non-repudiation.

Quercia and Hailes [20] came up with an idea for an electronic ticket system that could be used for mobile transactions. The system would make use of Chaum's blind signature approach [15] to issue limited-use and unlimited-use tickets. The privacy-preserving principal payments with refunds systems that were suggested by Rupp et al. [12], [21] were developed from Chaum's scheme [22] and the short signature technique that was proposed by Boneh et al. [23].

In their system, Chaum's blind forgeries were used to produce trip authorization tokens, while Boneh et alshort .'s signature method was utilised to perform the privacy-preserving aggregation of refunds. Both of these signature schemes were utilised. An electronic ticket scheme was proposed by Milutinovice et al. [3], which protects user privacy by combining three different schemes: the partial blind signature scheme proposed by Abe et al. [24], the secret sharing responsibility scheme proposed by Pedersen [25], and the anonymous credential scheme proposed by Camenisch et al. [26]. All of these other systems may keep user information private and provide unlinkability of tickets, however, in contrast to ours, they do not permit de-anonymization after double spending and they do not prevent tickets from being transferred.

Schemes for E-Tickets Generated by Group Signatures Using a group signature, a user is able to sign a message on behalf

of the group without revealing his name. The group manager, on the other hand, is able to reveal the identity of the person who really signed the message. Electronic coupons, or e-coupons, were proposed by Nakanishi et al. [27] as a method of providing anonymity and unlinkability via the use of a group signature technique [28]. An automated fare collecting (AFC) system was presented by Vives-Guasch [29] in which the group signature approach that was introduced by Boneh et al. [30] was utilised to guarantee unlinkability and revocable anonymity. Although these systems are capable of implementing anonymity, de-anonymity, ticket deniability, and ticket untransferability, they do not allow privacy-preserving attribute-based ticketing as our approach does.

Even though Gudymenko [10] addressed user privacy as well as differentially priced tickets in his e-ticket system, and even though he employed group signatures to make tickets unlinkable, no formal security models or security proofs were offered.

Schemes for Obtaining E-Tickets Using Anonymous Credentials Within the context of an anonymous credential scheme, a user is able to demonstrate to a verifier that she has a credential without disclosing any more information about herself. Heydt-Benjamin et al. [7] used anonymous credentials, e-cash, and proxy re-encryption methods in order to improve the security and privacy of their public transportation e-ticket systems. Arfaoui et al. [8] modified the signature scheme proposed by Boneh et al. in [31] to completely eradicate expensive bonding operational processes in the verification phase. After making this modification, they proposed a private information near field communication (NFC) mobile ticket (m-ticket) system by combining their modified certificate with the unidentified credential scheme proposed by Camenisch et al. [32]. This system could be used for mobile tickets. According to their plan, a user may only make an anonymous use of an m-ticket up to a maximum of k times before having that use cancelled by the revocation authority. Although these methods are capable of implementing anonymity, ticket unlinkability, and ticket untransferability, they do not, in contrast to our approach, enable privacy-preserving attribute-based ticketing. In addition to that, there was no concrete evidence that these strategies were secure.

Pseudonymous E-Ticket Scams and Their Origins Users are able to connect with numerous organisations anonymously and, in certain cases, without being linkable when they utilise pseudonyms. Fujimura and Nakajima [33] presented a framework for general-purpose e-tickets in which anonymity may be attained via the use of pseudonym schemes [34], [35]. Jorns et al. [36] suggested a pseudonym method that could be implemented on restricted devices. They then used this strategy to preserve the privacy of consumers while using e-ticket systems.

Kuntze and Schmidt [37] came up with a plan to construct pseudonym tickets by making use of the identities that were already included in attestation identity keys (AIKs) that had already been approved by the privacy certificate authority (PCA). Exculpability (i.e. a service provider cannot falsely accuse a user of having overspent her ticket, or the user is able to document that she has already validated the ticket before using it) and reusability (i.e. a ticket can be used a predefined number of times) were also addressed in the light-weight e-ticket scheme that was proposed by Vives-Guasch et al. [38]. This scheme used

pseudonyms Pseudonyms were employed in [38] to ensure that the transactions of users could not be linked to one another.

Kerschbaum et al. [11] took into consideration the privacy-preserving billing problem that arises with e-ticket systems, and they employed pseudonyms in order to offer unlinkability of user transactions. These methods are able to implement anonymity, the inability to connect tickets, as well as the inability to transfer tickets; but, unlike our approach, they do not enable privacy-preserving attribute-based ticketing.

In addition, there was no conclusive evidence that these strategies were safe to use.

Electronic Tickets Obtained from Special Devices Other electronic ticketing systems, such as personal trusted devices (PTD) [39], trusted platform modules (TPM) [37], mobile phones [40], and a variety of other options, are created around various specialised devices. These other techniques, in contrast to ours, call for the use of specialised hardware, do not provide deanonymization after the repeated use of a ticket, and do not provide support for privacy-preserving attribute-based ticketing.

In Table 1, we compare our scheme to other related schemes in terms of unlinkability, untransferability, double spend detection, de-anonymisation, attribute-based ticketing, and security proof. Whereas a indicates that the authors of the respective schemes did not consider security, our scheme is unlinkable, untransferable, detects double spend, de-anonymises users, and uses attribute-based ticketing.

Two standards on attribute-based encryption (ABE) have been produced by the European Telecommunications Standards Institute (ETSI) [41, 42]. These specifications may be used to safeguard personal data in a secure manner and to provide fine-grained access control. An ABE scheme encrypts a message by using a set of characteristics in such a way that only the users whose attributes match those in the ciphertext are able to decode it and see the message. This ensures that the message is kept secure. According to what is stated in [42], ABE is compatible with offline access restriction. On the other hand, our system only permits authentication via an online verifier, so users have that option. In addition, a user is able to demonstrate that she has essential qualities by using a given credential without having to expose those traits.

III CONSTRUCTION OF OUR SCHEME

In this part, we will discuss the structural components that make up our overall plan. Several ideas and concepts from other schemes, including Au et alsignature .'s with efficient protocol scheme [48], Camenisch et alset-membership .'s proof arrangement and price bracket proof scheme [47], Pedersen's commitment scheme [25], and Au et alscheme .'s for electronic cash [54], have been incorporated into our own. In particular, we included the signature strategy developed by Au et al., which allows a user to receive a signature on a committed block of attributes and show their knowledge of the signature using zero-knowledge. This was done by proving that the user has the signature.

This is to produce tickets for users as well as credentials for users and ticket sellers, and to provide credentials to users. In order to demonstrate a user's characteristics, we modify the set-membership proof and range proofs approaches presented in Camenisch et al.

[47]. Within the context of our system, these characteristics are also validated by an independent authority figure.

Pedersen's commitment scheme has been used in our system as a means of concealing the information that a prover is required to demonstrate. Last but not least, we implement the method proposed by Au et al. [54] to identify and deanonymize a double spend user.

Problems encountered in construction: Our architecture is based on the schemes given in [25], [47], [48], and [54]. The objective is to integrate and modify these schemes in such a way that the finished system includes the following three extra features: (1) The characteristics (such as age, handicap, etc.) that a user is required to verify to a ticket seller need to be validated by a trustworthy third party. If this is not the case, users might theoretically acquire reduced tickets using characteristics that they do not really possess. In order to circumvent this issue, the signature system developed by Au et al. [48] is used when certifying a user's characteristics. (2) Tickets must not be able to be transferred to another person or linked to another ticket, and there must be a way to detect duplicate spending.

Therefore, our tickets are produced using anonymously credentials, which contain an account and password but cannot be linked back to that user (transferability). A serial number is printed on each ticket in case the same person tries to use it more than once. The public trace approach that was presented by Au et al. in [54] is used to expose the user's identify (through her public key) if two tickets have always had the same serial number. (3) Both range policies that would ensure policies need to be accessible to users in order to achieve the desired level of adaptability in the process of policy configuration for tickets. Users are then able to use their certified attributes to demonstrate membership in multiple range and set policies, such as to get a young person discount, a frequent traveller bonus, as well as a disability reduction. For example, users can use their certified attributes to demonstrate membership in these types of policies.

High-Level Executive Summary

Both range rules and set policies may have an effect on the kind of tickets that can be purchased via our electronic ticketing system. Set policies may consist of numerous additional qualities, such as occupation, handicap, location, and so on, while range policies can contain attributes like age, number of travels made, pay, and so on. Both sets of policies can also comprise both range and set policies.

Setup. The process of setting up the scheme is shown in Figure 2. The authorities who regulate ticket prices The value of P will be equal to R1, , RN1, S1, , SN2 when it is first set.

where R1, S1, and RN1 represent the supported range policies and S1, S2, and SN2 represent the supported set policies, respectively. The CA chooses the following private keys. MSK = (x, y, 1, , N2) in which x is used to generate credentials for users of the system, y is used to generate tags identifying the range policies, and the I I = 1, , N2) are used to generate tags identifying the set policies. In this equation, x is used to generate credentials for users of the system, and y is used to generate tags identifying the range policies. After that, the CA will publish the public parameters params, which will contain the ticket price policy P, in addition to the range policy tags, and the set policy tags.

Registration. Figure 3 presents an overview of the many stages that make up

the registration process. The generation of a private-public key pair is a prerequisite for the registration of a seller, denoted by the letter S. (xs, YS). He demonstrates to the CA that he is aware of the secret key xs by transmitting YS along with a proof of knowledge in the form of 1 S. S supplies the CA with proof that he is authorised to function in the capacity of a seller by authenticating himself using an out-of-band communication channel. The certification authority (CA) creates a credential known as S, which is a BBS+ signature that incorporates the public key YS and a validity period known as V PS for the credential in the event that 1 S is legitimate and the authentication is successful. These particulars are then sent on to S, who validates the credential S in order to confirm that the CA has granted him permission to function as a vendor.

In the event of a user registration, a user U will produce a pair of secret and public keys denoted by xu and YU, and she will then submit her public key PU along with a proof of knowledge 1 U demonstrating that she is aware of the secret key xu. In addition to that, she gives the CA a list of the AU characteristics (such as age, occupation, area, and so on) that qualify her for a discount on the tickets. She authenticates herself to the CA once again by utilising an out-of-band channel, and she offers proof for the traits that she claims to have. If the conditions of Q1 U are met, the authentication process is successful, and the CA is pleased with the evidence that was presented, it will generate a credential known as U. This credential is a BBS+ signature scheme that contains the public key YU, the validity period V PU, and the attributes AU that correspond to it. These particulars are then sent back to U, who makes use of them in order to validate the claim that she is now a genuine user of the system and that the CA has validated her characteristics.

Ticket Issuing. The steps involved in the ticket-issuing process are broken below in Figure 4. Let PU be composed of the names of the many range polices and set polices that U has complied with. It is necessary for a seller S to demonstrate to a buyer U that he is authorised by the CA before the latter may purchase anything from the seller. This is done to stop attackers from gaining access to users' sensitive information. In order to accomplish this goal, a proof of knowledge 2 S of the seller's credential S must be constructed. If the proof is correct, the user U will continue by inventing a new pseudonym Y that includes her secret key xu and building a proof of knowledge 2 U of Y. If the proof is invalid, the user U will skip this step. This proof demonstrates to S that the CA has validated her identity as a genuine user by certifying that she has the stated qualities, which permit her to purchase the ticket that corresponds to the attributes that she has supplied. After S has successfully verified her proof, he will then construct a ticket TU using a BBS+ signature scheme. This scheme will include the user's pseudonym Y, the applicable range and set policies of the user that are relevant to the ticket, a serial number to enable double spend detection, as well as the price of the ticket and its validity period V PT. Note that although the ticket price and the period of time that it is valid for are both accounted for in the construction of TU, they are merely free text entries and should only be used when the application context necessitates the inclusion of price and validity periods. For example, if the validity period is significant, S should verify that the user's credential valid period V PU is at least as recent as the ticket valid period V PT and ensure that the ticket valid period V PT is

not earlier than V TU together with its related details is then delivered back to the user, who may use the information to verify the legitimacy of the information by combining it with the public key of the seller YS. It is important to keep in mind that our system ensures the unlinkability of tickets by virtue of the usage of user pseudonyms. This makes it impossible for the seller S or any verifier V to link any two tickets requested by the same user, even if they collude.

Ticket Validation. The process of validating a ticket is shown in Figure 5. Any verifier V's identification information may be stored in the table T ableU once it has been blankly initialised by the user U. This table's goal is to guarantee that a verifier may only request a ticket a single time in order to avoid a trustworthy user from having their anonymity compromised by an unethical verifier. On the other hand, the verifier V prepares an empty table known as T ableV to contain the authentication transcript received from the user authenticator U. This allows the verifier V to assess whether or not a ticket has previously been used (i.e. double spend detection). The verifier will first dispatch a brand new nonce r along with its identification IDV to the user before beginning the process of verifying the ticket. It is expected that there is some kind of out-of-band communication that enables the user to "authenticate" the verifier. For example, the verifier may be a guard on the train or a gate at the entrance to the station. The first thing that U does is make sure that V does not already have an entry in tableU. If there is already an entry, U will terminate the operation to prevent de-anonymization from occurring. In the event that this is not the case, she will submit V a "ticket transcript," sometimes referred to as T ransT, of her ticket T icketU, which will include a zero-knowledge proof of knowledge 3 U. The transcript ought to persuade V that she is an authorised user who is in possession of a legal ticket T icketU. Because TicketU incorporates the user's secret key xu as part of her pseudonym Y, knowledge of which has to be proved as part of 3 U. Our system guarantees that tickets cannot be sold or given away, supposing that U's private key has not been obtained by unauthorised parties. Additionally, in order to defend against even the most basic of replay assaults, the transcript includes V's nonce r. U finishes off her portion of the validation process by making the necessary changes to her TableU in order to store V's identification alongside r. If V is unable to properly verify U's ticket transcript, then V will deny the request. In the event that V is successful in verifying U's ticket transcript, then V will provide her access to the service and update T ableV with T ransT.

Identifying Cases of Double Spending The procedure for identifying double spending is shown in Figure 6. V examines TableV for another ticket transcript T ransU with the same serial number D to determine whether or not a ticket is being double spent. If there is, then the ticket is being doubly spent, and V will be able to de-anonymize U by extracting her public key YU from the two transcripts; if there isn't, then it is a brand new ticket.

It is important to highlight the fact that the implementation of our plan comes with the following supplementary advantage.

Updates to the Dynamic Policy are Restricted. If the seller S needs to either create new policies in P or update some existing ones, he can contact the central authority CA to either update or create the relevant public parameters params. As a consequence of this, a user U can prove to S that his attributes satisfy the updated

policies by using the updated params when purchasing a ticket, and S will generate tickets according to the updated policies. If U's existing characteristics no longer meet the requirements of the revised regulations, then the CA will need her to receive new credentials from them.

Take, for instance, Alice, who we will assume is 16 years old. If the buyer S demands that the current policy range of [12, 18] be adjusted to [15, 20] instead, then Alice will still be able to utilise the credentials she has already established. On the other hand, if the policy were to be altered from [12, 18] to [18, 25], then Alice would be required to get in touch with the CA in order to have her credentials updated.

Correctness. The comprehensive edition of this work [55] provides evidence that demonstrates how accurate our system is.

IV BENCHMARKING RESULTS

In this part of the article, we will analyse how well our plan worked.

The implementation's source code can be found at [56], and its performance was evaluated using a laptop running Fedora 27 and a Dell Inspiron Latitude E5270 equipped with an Intel Core i7-6600U CPU, a 1TB SSD, and 16GB of RAM. The source code is accessible online. The implementation takes use of a variety of cryptographic primitives, including bilinear maps constructed over elliptic curves, amongst other options.

We made use of the JPBC library [57] in order to generate the bilinear maps, and we relied on bouncycastle [58] to generate the other cryptographic elements that were necessary for our method. It is important to take note that the Java-based version of the JPBC API [57] was used throughout.

You may recall from Section 2 that our strategy necessitates the use of a Type I symmetric bilinear map, denoted by the notation e: G GG. The JPBC library [57] includes three distinct examples of a symmetric pairing with their Type A, A1 or E pairings.

The Type A and A1 pairings are based on the elliptic curve E: y 2 = x 3 + x over the finite field Fp. The Type E pairings are based on the elliptic curve E. In both instances, the group denoted by G is the same as the group denoted by E, which is the elliptic curve (Fp). The complex multiplication (CM) technique is used to generate elliptic curves, and it begins with the Diophantine equation DV 2 = 4p t 2 as its point of departure. On the other hand, the Type E pairing is based on this approach. [59] provides more information on each individual structure.

During the instantiation of the various pairings in our implementation, we make use of the default parameters. For example, Type A is constructed with rBits = 160 and qBits = 512; Type A1 uses 2 primes of size qBits = 512; and Type E is instantiated with rBits = 160 and qBits = 1024. All of these parameters are taken from the documentation.

Note that according to Table 1 in [60], JPBC's default Type A pairing offers about the same level of security as 80-bit symmetric or 1024-style RSA encryption. This is enough for the purpose of establishing a baseline from which to take time measurements.

For the hash functions H: 0, 1 Zp and H0 : 0, 1 G that are needed by our scheme (see Fig. 2), we utilised SHA256 for H, and we relied on the implementation of the "newElementFromHash()" method in the JPBC library for H0. Both of these hash functions are required by our scheme.

However, range proofs have an additional advantage, which is best shown by an illustration: the age of a young person may be specified either in a range policy (age [15, 25]) or with a set policy ("young person"). Our plan gives those in charge of policymaking the ability to exercise discretion over the kind of policies that should be implemented.

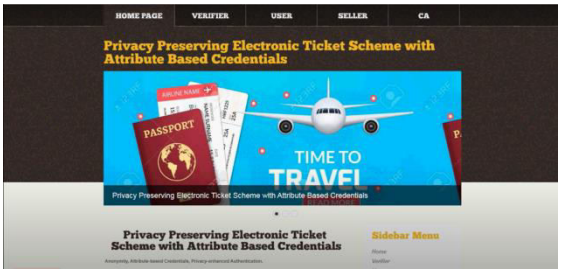
The computational efficiency of a set policy is much higher than that of a range policy; nevertheless, range policies have the capacity to accept future policy revisions. Specifically, let's say that Alice is 23 years old. Since the young person range policy at the moment is supplied by age [16, 22], it follows that Alice is not eligible for a discount of any kind.

Alice is able to continue to utilise her current age attribute of 23 to earn a young person discount even if it is subsequently altered to age [16, 25]. This is because she is now able to demonstrate that her age fits within the revised range.

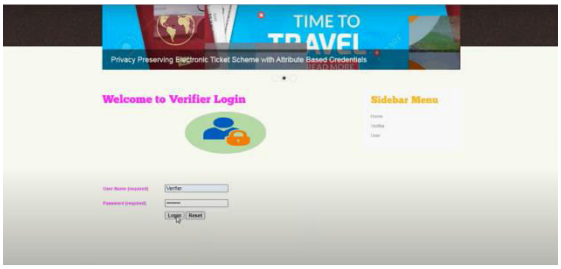
However, if the set policy method had been used, Alice would have been ineligible for the signed "young person" characteristic in the past. As a result, she would have been required to return to the CA in order to have her credentials updated.

Therefore, for any actual system, it is vital to look at the trade-off between the flexibility that range policies enable in terms of dynamic updates and their more costly computational cost. In other words, it is important to keep an eye at the range policies' impacts of the event adaptability.

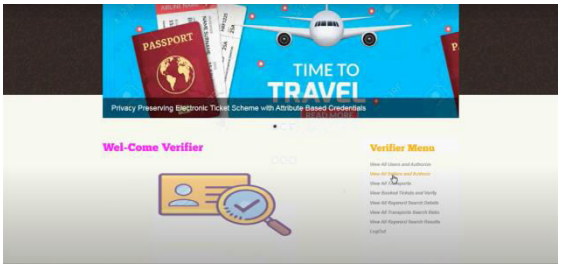
V RESULTS



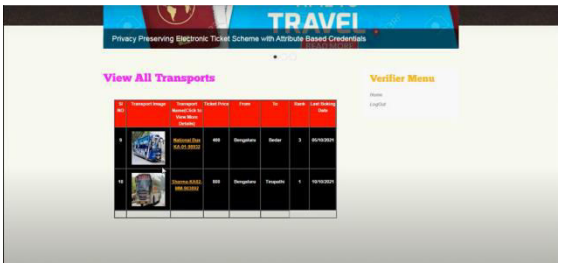
Home Page



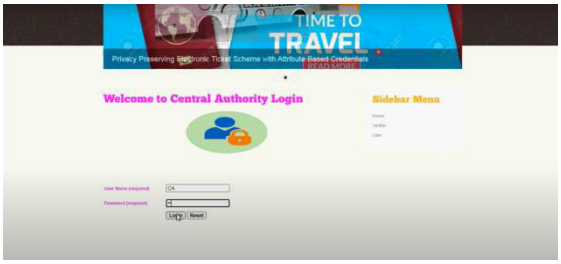
Verifier Login Page



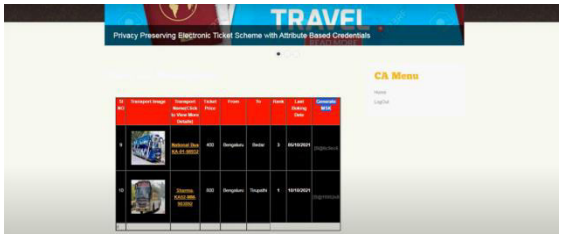
Welcome Verifier



View all Transport

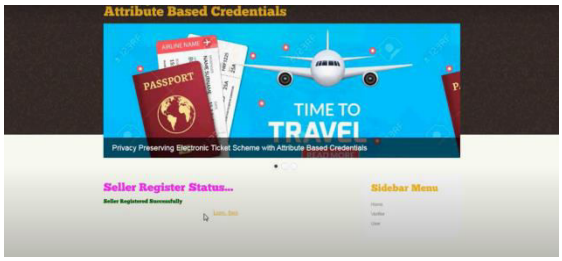


Authority Login

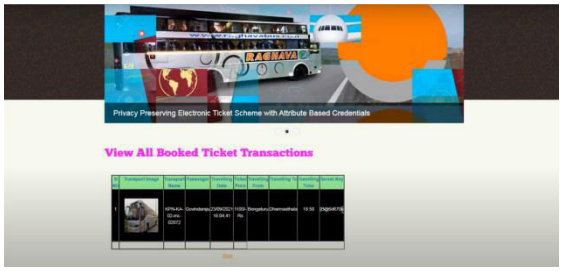


CA Menu

Seller Registration



Seller Registration



Booked Transcations

VI CONCLUSIONS AND WORK TO BE DONE IN THE FUTURE

Several different methods have been presented in order to preserve the privacy of users inside e-ticket schemes; however, these schemes do not solve attribute-based ticketing. In a similar manner, privacy-preserving attribute-based credentials schemes have been developed, whereby attributes may either be elements of a set or within a range; however, this work presents a method that can enable both the usage of sets and ranges inside the same scheme. This kind of method, together with its security model and proof of security, has been outlined in the article. One of the advantages of implementing this plan is that it gives decision-makers the latitude to choose the kind of policies that should be put into effect. Set policies are more efficient from a computational standpoint than range policies are, but range policies have the ability to accept new rules in the future. Due to the high cost of computation and the increased communication overhead, our system is not yet suited for portable devices such as smart phones, tablets, and the like at this time.

In our future work, we will investigate the impact that allowing dynamic policy updates has on the security model and the proof, and we will also make modifications to the deployment of the system in order to improve its performance. For example, we might pre-compute static values whenever it is possible, and we might use the C-based PBC library [61], but we might also consider offshoring arithmetic operations [62], [63], substantiated outsourcing arithmetic operations [64], [65], [66], etc.

REFERENCES

[1] United Airlines. (2017) Customer data privacy policy. [Online]. Available: https://www.united.com/web/en-US/content/ privacy.aspx

[2] Rail Delivery Group. (2017) Rail technical strategy capability delivery plan. [Online]. Available: https://www.rssb.co.uk/rts/Documents/ 2017-01-27-rail-technical-strategy-capability-delivery-plan-brochure. pdf

[3] M. Milutinovic, K. Decroix, V. Naessens, and B. D. Decker, “Privacy-preserving public transport ticketing system,” in DBSec’15. Springer, 2015, pp. 135–150.

[4] M. Mut-Puigserver, M. M. Payeras-Capella`, J.-L. Ferrer-Gomila, A. Vives-Guasch, and J. Castella`-Roca, "A survey of electronic ticketing applied to transport," Computers & Security, vol. 31, no. 8, pp. 925–939, 2012.

[5] A. Vives-Guasch, M. M. Payeras-Capella`, M. Mut-Puigserver, J. Castella`-Roca-Roca, and J.-L. Ferrer-Gomilas, "Anonymous and transferable electronic ticketing scheme," in DPM'13 and SETOP'13. Springer, 2013, pp. 100–113.

[6] (2016) General Data Protection Regulation. [Online]. Available: https://eugdpr.org/

[7] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, "Privacy for public transportation," in PET'06. ACM, 2006, pp. 1–19.

[8] G. Arfaoui, J.-F. Lalande, J. Traore´, N. Desmoulins, P. Berthome´, and S. Gharout, "A practical set-membership proof for privacypreserving NFC mobile ticketing," in PoPETs'15. DE GRUYTER, 2015, pp. 25–45.

[9] R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection," IEEE Transactions on Consumer Electronics, vol. 49, no. 2, pp. 408–413, 2003.

[10] I. Gudymenko, "A privacy-preserving e-ticketing system for public transportation supporting fine-granular billing and local validation," in SIN'14. ACM, 2014, pp. 101–107.

[11] F. Kerschbaum, H. W. Lim, and I. Gudymenko, "Privacypreserving billing for e-ticketing systems in public transportation," in WPES'13. ACM, 2013, pp. 143–154.

[12] A. Rupp, G. Hinterwa¨lder, F. Baldimtsi, and C. Paar, "P4r: Privacypreserving pre-payments with refunds for transportation systems," in FC'13. Springer, 2013, pp. 205–212.

[13] IATA. (2012) Transferability of tickets. [Online]. Available: https://www.iata.org/policy/Documents/Transferability.pdf

[14] B. Patel and J. Crowcroft, "Ticket based service access for the mobile user," in MobiCom'97. ACM, 1997, pp. 223–233.

[15] D. Chaum, "Blind signatures for untraceable payments," in Crypto'82. Springer, 1982, pp. 199–203.

[16] D. Chaum and E. van Heyst, "Group signatures," in EUROCRYPT'91. Springer, 1991, pp. 257–265.

[17] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," Communications of the ACM, vol. E28, no. 10, pp. 1030–1044, 1985.

[18] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," in SAC'99. Springer, 1999, pp. 184–199.

[19] C.-I. Fan and C.-L. Lei, "Multi-recastable ticket schemes for electronic voting," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E81-A, no. 5, pp. 940– 949, 1998.

[20] D. Quercia and S. Hailes, "Motet: Mobile transactions using electronic ticket," in SecureComm'05. IEEE, 2005, pp. 1–10.

[21] A. Rupp, F. Baldimtsi, G. Hinterwa¨lder, and C. Paar, "Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport," ACM Transactions on Information and System Security, vol. 17, no. 3, pp. 10:01–10:31, 2015.

[22] S. Brands, "Untraceable off-line cash in wallets with observers (extended abstract)," in CRYPTO'93. Springer, 1993, pp. 302–318.

[23] D. Boneh, B. Lynn, and H. Shacham:, "Short signatures from the weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.